What is claimed is:

1. A method for conducting authenticated business transactions involving microprocessor equipped devices over a distributed network, the method comprising the acts of:

a) providing an on-line authentication service available on the distributed network;

b) authenticating a plurality of users to said on-line authentication service using a closed authentication system to produce a plurality of authenticated users; and

c) connecting a group of at least two of said plurality of authenticated users under persistent mediation of said on-line authentication service, producing a connected group.

2. The method of claim 1 further comprising enrolling said users to said on-line authentication service prior to authenticating said users to said on-line authentication service.

3. The method of claim 2 wherein persistent mediation of said connected group comprises compiling an audit trail of an interaction of said connected group.

4. The method of claim 3 wherein said closed authentication system is a pseudo-PKI system of the type which cryptographically camouflages a user's private key in a software container.

5. The method of claim 4 wherein the on-line service is a persistent authentication and mediation service.

6. A method for conducting authenticated business transactions involving microprocessor equipped devices over a distributed network, the method comprising the acts of:

a) providing an on-line authentication service available on the distributed network;

b) authenticating a plurality of users to said on-line authentication service using a closed PKI authentication system to produce a plurality of authenticated users; and

c) connecting a group of at least two of said plurality of authenticated users under persistent mediation of said on-line authentication service, producing a connected group.

7. The method of claim 6 further comprising enrolling said users to said on-line authentication service prior to authenticating said users to said on-line authentication service.

8. The method of claim 7 wherein persistent mediation of said connected group comprises compiling an audit trail of an interaction of said connected group.

9. The method of claim 7 wherein said closed PKI authentication system is a pseudo-PKI system of the type which cryptographically camouflages a user's private key in a software container.

10. The method of claim 9 wherein the on-line service is a persistent authentication and mediation service.

11. A method for conducting authenticated business transactions involving microprocessor equipped devices over a distributed network, the method comprising the acts of:

a) providing a persistent authentication and mediation service as an on-line service on the distributed network;

b) enrolling users seeking enrollment in the persistent authentication and mediation service, to produce a plurality of enrolled users;

c) receiving requests from enrolled users for authentication to the persistent authentication and mediation service;

d) authenticating enrolled users seeking authentication to the persistent authentication and mediation service using a closed PKI authentication system, so as to maintain a plurality of authenticated users;

e) receiving requests from authenticated users to be connected to particular other authenticated users;

f) connecting groups of at least two authenticated users under persistent mediation of the persistent authentication and mediation service so that the at least two authenticated users can conduct an interaction;

g) repeating act (f) to produce a plurality of groups of connected users; and

h) mediating the interaction among the at least two users of each of said plurality of groups of connected users after connection, wherein the act of mediating the interaction comprises the acts of providing authenticated identity information to the interaction, directly compiling an audit trail of the interaction and making information from the audit trail available to the at least two users of each group of connected users.

12. The method of claim 11 wherein the act of enrolling users seeking enrollment in the persistent authentication and mediation service comprises the acts of:

a) distributing software to a user seeking enrollment which enables microprocessor equipped devices operated by the user seeking enrollment to interact with said persistent authentication and mediation service,

b) generating a unique private key, and a unique public key for the user seeking enrollment,

c) obtaining permanent credentials particular to each of the user seeking enrollment, said credentials comprising public permanent credentials and secret permanent credentials,

d) deciding whether to approve the applicant seeking enrollment;

e) distributing the unique public key and the unique private key to the user seeking enrollment if the user seeking enrollment is approved, and

f) storing said permanent credentials in a customer database, said customer database being accessible to said persistent authentication and mediation service, whereby the user seeking enrollment becomes one of said multiplicity of enrolled users, and

g) repeating steps (a) through (f) for each applicant seeking enrollment.

13. The method of claim 12 wherein the act of authenticating enrolled users seeking authentication to the common authenticating service comprises the acts of:

a) generating a challenge message from the persistent authentication and mediation service and sending it over the public network to an enrolled user seeking authentication,

b) receiving a response to the challenge from the user seeking authentication, said response comprising an encrypted message and the unique public key unique to the enrolled user seeking authentication,

c) verifying the authenticity of the response to the challenge, the act of verifying the authenticity comprising the act of decrypting the response using the public key unique to the enrolled user seeking authentication to produce a decrypted response,

d) authenticating the enrolled user seeking authentication if the decrypted response indicates that the response was authentic, whereby the enrolled user seeking authentication becomes an authenticated user,

e) rejecting the user if the decrypted response indicates that the response was not authentic, and

f) repeating steps (a) through (e) for each enrolled user seeking authentication.

14. The method of claim 13 further comprising the acts of:

a) allowing authenticated users to optionally submit variable credentials;

b) receiving variable credentials submitted by authenticated users;

c) storing the variable credentials in the customer database according to user;

d) providing authenticated users discovery software, whereby authenticated users may dynamically discover enrolled users according to search criteria.

e) granting authenticated users access to search the public permanent credentials and the variable credentials in the customer database, using said discovery software.

15. The method of claim 14 further comprising making available collaboration software to each of said plurality of groups of connected users is to facilitate communication among the at least two authenticated users of each group, wherein said collaboration software makes information from the audit trail available to each of said at least two authenticated users of each of said plurality of groups of connected users.

16. The method of claim 15 wherein:

a) the software PKI authentication system is a pseudo-PKI system of the type which cryptographically camouflages the unique private keys in a software container,

b) wherein the unique public keys is encrypted in a form recognizable to the common authentication agent and stored in a digital certificate,

c) wherein the act of authenticating an enrolled user to the common authenticating service further comprises the act of decrypting the encrypted

unique public key unique to the enrolled user prior to decrypting the response.

17. The method of claim 16 wherein the persistent authentication and mediation service is provided by at least one host site connected to the distributed network, said at least one host site comprising at least one computer server operated by an open software platform providing intelligent interactions, wherein the operation the persistent authentication and mediation service is implemented by software operating on the open software platform.

18. The method of claim 17 wherein interactions between users and the persistent authentication and mediation service are mediated through the open software platform.

19. The method of claim 18 wherein some of the plurality of groups of connected users comprise at least three authenticated users.

20. The method of claim 19 wherein some of the plurality of groups of at least three connected users comprise users of different types.

21. The method of claim 18 wherein the distributed network is the public Internet.

22. An online service for conducting business transactions among microprocessor equipped devices over a distributed network, the online service comprising:

a) a host site connected to the network, the host site comprising an open software platform providing intelligent interactions;

b) a persistent authentication and mediation service, the persistent authentication and mediation service comprising a software PKI authentication agent operating on said open software platform such that

communications over the network by said persistent authentication and mediation service are mediated by said open software platform;

c) a customer database comprising permanent credentials and dynamically variable information corresponding to users of the online service and a database manager for managing the customer database;

d) software operating on said open software platform which performs at least the following functions:

i) enrolling users seeking enrollment in the persistent authentication and mediation service to produce enrolled users,

ii) storing credentials corresponding to enrolled users in the customer data base,

iii) authenticating enrolled users seeking authentication to the persistent authentication and mediation service to produce authenticated users,

iv) allowing a authenticated users to discover enrolled users according to search criteria,

v) allowing authenticated users to be connected under mediation of the persistent authentication and mediation service through the open software platform,

vi) allowing collaboration between authenticated users which have been connected, and

vii) memorializing transactions between authenticated users.

23. The online service defined in claim 22 where the function of enrolling users seeking enrollment in the persistent authentication and mediation service comprises the functions of:

a) distributing software to a user seeking enrollment which enables microprocessor equipped devices operated by the user seeking enrollment to interact with the persistent authentication and mediation service,

b) generating a unique private key, and a unique public key for the user seeking enrollment,

c) obtaining permanent credentials particular to each of the user seeking enrollment, said credentials comprising public permanent credentials and secret permanent credentials,

d) deciding whether to approve the applicant seeking enrollment;

e) distributing the unique public key and the unique private key to the user seeking enrollment if the user seeking enrollment is approved, and

f) storing said permanent credentials in a customer database, said customer database being accessible to said persistent authentication and mediation service, whereby the user seeking enrollment becomes one of said multiplicity of enrolled users, and

g) repeating steps (a) through (f) for each applicant seeking enrollment.

24. The online service defined in claim 23 wherein the function of authenticating enrolled users seeking authentication to the persistent authentication and mediation service comprises the functions of:

a) generating a challenge message from the persistent authentication and mediation service and sending it over the public network to an enrolled user seeking authentication,

b) receiving a response to the challenge from the user seeking authentication, said response comprising an encrypted message and the unique public key unique to the enrolled user seeking authentication,

c) verifying the authenticity of the response to the challenge, the act of verifying the authenticity comprising the act of decrypting the response using the public key unique to the enrolled user seeking authentication to produce a decrypted response,

d) authenticating the enrolled user seeking authentication if the decrypted response indicates that the response was authentic, whereby the enrolled user seeking authentication becomes an authenticated user,

e) rejecting the user if the decrypted response indicates that the response was not authentic, and

f) repeating steps (a) through (e) for each enrolled user seeking authentication.

25. The online service defined in claim 24 wherein:

a) the software PKI authentication agent is a pseudo-PKI system of the type which cryptographically camouflages each of the unique private keys in a software container,

b) wherein each of the unique public keys is encrypted in a form recognizable to the common authentication agent and stored in a digital certificate,

c) wherein the function of authenticating an enrolled user to the common authenticating service further comprises the function of decrypting the encrypted unique public key unique to the enrolled user prior to decrypting the response.

26. The online service defined in claim 25 wherein the distributed network is the public Internet.

27. A system for conducting business transactions over a distributed network, the system comprising:

a) a persistent authentication and mediation service site providing a persistent authentication and mediation service, said site connected to the public network, said site comprising

i) a open software platform application providing intelligent interactions said platform application mediating all interactions of said persistent authentication and mediation service site via said public network,

ii) anauthentication agent application comprising a software pseudo-PKI authentication application operating on said open software

platform application, said common authentication agent application comprising software which enrolls new businesses users producing enrolled users and authenticates the enrolled users,

iii) an audit agent application operating on said open software platform which logs and monitors interactions mediated by the open software platform,

iv) a discovery software application operating on said open software platform, and

v) a collaboration software application operating on said open software;

b) a multiplicity of user sites operated by the enrolled users, the user sites being connected to the public network, each site operating at least one computer application whereby it may interact with other business users and each site further comprising software which allows interaction with the persistent authentication and mediation service, a software camouflaged private key, and a digital certificate, said digital certificate comprising an encrypted pseudo-public key recognizable to said persistent authentication and mediation service;

c) a database of authentication information pertaining to the enrolled business users of said persistent authentication and mediation service, the database accessible to the common authentication application.

28. The system defined in claim 27 further comprising a plurality of authentication provider applications accessible by the authentication agent application.

29. The system defined in claim 28 wherein at least one authentication provider application is located at a different site than the persistent authentication and mediation service site.

30. The system defined in claim 28 further comprising a plurality of audit provider applications accessible by the audit agent application.

31. The system defined in claim 29 wherein at least one authentication application provider is located at a different site than the persistent authentication and mediation service site.

32. The system defined in claim 29 wherein the network is the public Internet.

33. The system defined in claim 31 wherein the network is the public Internet.

34. The system defined in claim 33, wherein the user sites comprise sites which are chosen from the group consisting of user sites which access the network via a browser operating on a computer, mobile telephonic devices which access the network, world wide web sites, and sites comprising applications without a user interface.

35. An apparatus for providing a service for conducting authenticated business transactions involving a multiplicity of users over a distributed network, the apparatus comprising:

a) at least one application server connected to the public network, the at least one application server having a computer processor and a computer readable memory, the memory storing the software to implement the service, the software comprising

i) an open software platform providing intelligent interactions,

ii) a software pseudo-PKI authentication agent application, operating on said open software platform,

iii) a discovery software application, operating on said open software platform, and

iv) a collaboration software application, operating on said open software platform,;

b) at least one database server, the at least one database server comprising a business users database, the business users database comprising

i) authenticated data about registered business users, said authenticated data being protected from user modification;

ii) data pertaining to registered business users which is dynamically modifiable by said business users; and

iii) data needed for linking business users;

whereby the application server facilitates authenticated interactions between business users, including the ability to access other authenticated users without repeated logging in, the ability to dynamically search for authenticated users according to user defined specifications, and accomplish peer to peer collaboration.

36. An apparatus as defined in claim 35 where the distributed network is the Internet.